OIT-0261-88

24 MAR 1988

25X1

MEMORANDUM FOR: [redacted]
Chief, Information Management Staff, DO

FROM: Edward J. Maloney
Director, Office Information Technology, DA

SUBJECT: Request for Immediate Program Modifications to
Clear all Splits During Log Off

REFERENCE: Your Memo, dtd 1 Feb 88, Same Subject

1. I have directed the appropriate members of OIT's Engineering Group to contact your Information Security Staff to review the requirements for such modifications. OIT is well aware of the implications of the split screen capability of Delta Datas and has exhaustively studied this particular situation several times. It has been the subject of correspondence between our offices, at least at the staff level, most recently an exchange via AIM in October, 1986. Since that time, even more reasons can be expressed for recommending no action. I will summarize the analyses again for the record, but I am confident that, after reviewing the previous discussions, your staff will again conclude that no action is warranted. [redacted] 25X1

2. In brief, the reason that no action has ever been taken is that the threat in this regard has historically been only from particularly privileged individuals -- primarily those on your staff who both have access to sensitive data and logon passwords to the [redacted] Center. Our analysis has been that the threat of such individuals egregiously violating policy in moving data via this mechanism and furthermore conspiring with others in the [redacted] Center to exploit such a path is clearly inconsequential compared to any number of other threats that such overtly hostile, trusted employees represent. The memory of the terminal is merely an automated aid to writing down information and re-keying it into the other, also classified, access-controlled center, not a fundamentally new and valuable tool of tradecraft worth risking exposure to exploit. [redacted]

25X1 25X1 25X1

25X1

[redacted]

[redacted]

SUBJECT: Request for Immediate Program Modifications to Clear all Splits During Log Off

3. The preferred policy of both our offices has been to limit the number of people with access to both centers, and I feel that this should continue. 25X1 With [redacted] users having dual accesses, your concern is magnified beyond what it was when it was mainly IMS and OIT personnel who had dual accesses. I would recommend that, since you view isolation as a mandatory requirement, such dual accesses be reviewed very carefully. If there are needs to communicate with other directorates, perhaps we should discuss a more appropriate means than dual access by so many people. An audited, electronic mail link, such as actually already exists via the cable network, might be much more appropriate 25X1 than increasing the number of people with dual accesses. [redacted]

4. Notwithstanding these analyses, it is technically possible to have the system try to clear all splits at logoff. Unfortunately, this has the effect of removing one of the more valuable fail-safe mechanisms that customers have of saving data, making it more likely that work will be lost in Host-Based Word Processing, for example, when the systems have problems. Furthermore, the attempt by the host to clear the splits can generally be defeated by the sort of knowledgeable user who would be the only one to try to exploit this mechanism in the first place. Data is neither retained in splits automatically, nor transferred up to host without deliberate knowledge and effort. A few more terminal commands can defeat any attempt by the host to clear memory. There are even simpler, mechanical means to block the attempt by the host to clear memory. Thus the cost/benefits tradeoff of attempting to address this problem by program modifications to the host operating systems 25X1 argues strongly against such modifications. [redacted]

5. Your memo also addresses the issue of PC memory and its potential for expanding the referenced vulnerabil ty. PCs will indeed increase the amount of memory available many times over However, the difference is still merely one of degree, not a new threat. M eover, there is technically no way for the host to clear the PC's memory a all, nor do we ever expect there to be one. While OIT could entertain a r quest to attempt (without guarantee of success) to clear Delta Data splits no such request for PCs can ever be 25X1 contemplated. [redacted]

6. After reviewing the issue, please let me know if there are any actions that you still view as being desir ble. If there are any questions, please 25X1 contact [redacted] of OIT/Engineerin; Group [redacted]

25X1 [redacted]

for Edward J. Maloney

SUBJECT: Request for Immediate Program Modifications to Clear all Splits During Log Off

25X1 DA/OIT/EG [redacted] (4 MAR 88)

Distribution:

Original - addressee
1 - D/OIT
1 - EG CHRONO
1 - OIT Reg

SECRET

MEMORANDUM FOR: Director of Information Technology

25X1

FROM: [redacted]
Chief, Information Management Staff, DO

SUBJECT: Request for Immediate Program Modifications to Clear all Splits During Log Off

1. In order to regain the isolation of the Special Center, I am requesting an immediate change to those system programs which control the terminal log off functions. The change must clear all terminal memory, including splits, before conclusion of the log off command.

2. I have recently witnessed a demonstration of the vulnerability of the split screen capability, allowing unauthorized movement of data from one computer center to another. This vulnerability weakens the logical isolation of the Special Center and violates the concept of the one-way-data-link.

3. The current log off command allows the capability to save data in one or more areas of the terminal memory buffer, called "splits." When issuing the log off command from one computer center (Special), data is stored within this buffer. After logging on to a second computer center [redacted] the stored data is easily transferred, using a few simple terminal display commands, to the split set up explicitly for this center. The data then can be stored, altered, or sent to users not authorized access to the Special Center. The Delta Data terminals in use throughout the DO have buffers large enough to allow the transfer of significant quantities of data at one time. PC terminals will have even greater buffers.

25X1

25X1

4. At present, there are [redacted] Special Center users who also have access to the [redacted] Center and a few with access to Northside.

25X1

25X1

[redacted]

SECRET

This list will grow as the need to communicate with the other directorates increases. There is no audit or logging executed when using this capability, nor is there any way to monitor the subject or classification of the data transferred.

5. Please contact Chief, IMS/Information Security Staff

25X1 [redacted] with any questions which you might have in regard to this request.

25X1

[redacted]

2 March 1988

STAT

MEMORANDUM FOR: [redacted]

FROM:

SUBJECT: Delta Data Security Memo

Attached, for your reference only, is a record of the most recent previous exchange between IMS and EG staff on the same subject. This previous exchange is only one of a series, as this problem resurfaces about every two years. The last time, we successfully convinced IMS not to pursue this issue. C/IMS did receive copies of this discussion at the time, but did not retain them. IMS Security Staff, [redacted] in particular, did retain this exchange on AIM, but unfortunately "rediscovered" the problem and forgot that we had addressed it before.

STAT

In answering this memo formally, I hope that this is the last time the issue comes up.

STAT

[redacted]

CONFIDENTIAL

DATE: October 29, 1986

25X1 NOTE TO: [redacted]

SUBJECT: Security and the Delta Data

Tom:

25X1 [redacted] just called and asked me about the status of a potential security problem involving multiple splits in the Delta Data. I had never heard of the problem or thought about it before, but anyway, here is the scenario:

25X1 (1) I want to transfer data from the Special Center to the [redacted] Center without the trace of a tape transfer.

(2) I set up my Delta Data for two splits, log onto the Special Center in split 1 and read data into the terminal's buffer for split 1.

(3) I then log off of the Special Center (my split 1 buffer is not
25X1 disturbed) and log onto the [redacted] Center in split 2. Now I can
25X1 move the split 1 data to split 2 and store it on the [redacted] Center system, thereby subverting the one-way-link protocol.

Have you ever heard of this potential problem before? How about a fix (DD short-stops logoff, mainframe sends down a flush buffer command at logoff)?

25X1 [redacted]

CONFIDENTIAL

RESPONDING TO: [redacted]

RE: (et al.) note dated 10/29/86

Yes, I am well aware of that "problem". It has been the subject of much discussion over the years and has probably been included in one or more formal memos at some point, though I cannot put my hands on any.

My advice, which has always carried the day in NSEG, is that this is red herring, at most a personnel security issue and not a technical one. The scenario describes a willful act by a very knowledgeable person with both Special and [redacted] Center access -- i.e. one of the handful of people in IMS/SG or NSEG. Furthermore, the amount of data moved in this fashion vs. the level of knowledge and effort require to accomplish it represent an inconsequential threat. The process described is extraordinarily difficult and moves across a few screens full of data at the most and allows the violator to do no more than he could by writing down the data from one system and just re-keying it into the other. Any of the people with the dual access and the knowledge to go through this hokey method would be a lot more dangerous than this silly threat represents if they were "bad".

To answer your question, there are some things that could be done to make life a little harder on the folks, but nothing foolproof. We only send out a "clear split" on LOGOFF, whereas we could send out a "clear all splits". I'm sure IMS has asked that of NSEG before several times and always been dissuaded. We wouldn't do this for all centers because customers have a valid need in some cases to put data aside in offline splits, especially when the system is flakey for example. Clearing all splits would make it tough on WP users to recover from a number of problems without losing their changes. If the DO ever really insisted on having a special version of VM that did do "clear all splits" just for them, it probably could be done, but the damage done would outweigh the benefits.

This is because the benefits are zero! Someone intent on moving data between centers can trivially defeat either or both types of split clear sequences. You have to keep in mind not the technical "problem" but instead the threat model. Having assumed a motivated and very very knowledgeable person, defeating the host's attempt to clear all the splits is as little as only one more keystroke!!! Only absolutely denying dual access by the same terminal makes any appreciable improvement in closing this "hole".

I understood IMS's position on the PBX to be taking this step, actually, and not allowing data calls to the [redacted] Center anymore. If this old bugaboo is the rationale behind that, I'm certainly disappointed in that judgement. I am particularly unimpressed that we are still discussing security features of Delta Datas which aren't even being bought anymore, while the horrendous security issues related to PCs are staring us in the face with little progress evident. I hope we can have some more fruitful discussions in that arena soon.

CONFIDENTIAL

25X1

RESPONDING TO: [redacted]

RE: (et al.) note dated 10/29/86

George,

Do you have to log-off one split before logging onto another center from the second split????

B.C.

CONFIDENTIAL

25X1

RESPONDING TO: [redacted]

RE: reply dated 10/30/86

Bob:

Yes. The Delta Data has only one physical connection (port) to a computer. There is no way in our environment that it can be multiplexed (more than one logical channel on a single physical channel).

Tom:

Is the above true categorically for the Delta Data or is it that we use only one port?

25X1 [redacted]

CONFIDENTIAL

CONFIDENTIAL

25X1 RESPONDING TO: [redacted]

RE: reply dated 10/31/86

You can say that it is true categorically for the Delta Data because the firmware only supports one host port. In TTY mode, there is no multiplex protocol to allow multiple logons (whereas there is in 3270 DFT). In SAFE, we support multiple contexts over TTY lines, but only the one user is logged on and only once -- just doing various things within his own virtual machine at the same time.

25X1 (We prevent multiple logon 3270 between Special and [redacted] at the same time by not providing "pass-thru" or SNA terminal links between the centers as part of the one-way restriction philosophy.)

CONFIDENTIAL